Fast Computation of the Nth Term of an Algebraic Series over a Finite Prime Field

Alin Bostan [1] Gilles Christol [2] Philippe Dumas [1]

[1]Inria (France)

[2]Institut de mathématiques de Jussieu (France)

Specfun Seminar, June 2016

Motivation

- Ubiquity: combinatorics, number theory, algebraic geometry

Motivation

- Ubiquity: combinatorics, number theory, algebraic geometry

- Confluence of several domains:
  - functional equations
  - automatic sequences
  - complexity theory

Motivation

- Ubiquity: combinatorics, number theory, algebraic geometry

- Confluence of several domains:
  - functional equations
  - automatic sequences
  - complexity theory

- *One of the most difficult questions in modular computations is the complexity of computations mod p for a large prime p of coefficients in the expansion of an algebraic function.*

D. Chudnovsky & G. Chudnovsky, 1990

Computer Algebra in the Service of

Mathematical Physics and Number Theory

Problem and main result

Input:

- prime field $\mathbb{K} = \mathbb{F}_p$
- $E(x, y) \in \mathbb{K}[x, y]$, with $E(0, 0) = 0$, $E_y(0, 0) \neq 0$
- $N \in \mathbb{N}$

Output:

- the Nth coefficient of the unique solution $f(x) \in \mathbb{K}[[x]]$ of $E(x, f(x)) = 0$, $f(0) = 0$

Problem and main result

Input:

- prime field $\mathbb{K} = \mathbb{F}_p$
- $E(x, y) \in \mathbb{K}[x, y]$, with $E(0, 0) = 0$, $E_y(0, 0) \neq 0$
- $N \in \mathbb{N}$

Output:

- the Nth coefficient of the unique solution $f(x) \in \mathbb{K}[[x]]$ of $E(x, f(x)) = 0$, $f(0) = 0$

Main result:

- arithmetic complexity linear in $\log N$ and almost linear in p

State of the art

First N coefficients complexity at best $\Theta(N)$

Chudnovsky + Chudnovsky, 1986
On expansion of algebraic functions in power and Puiseux series, I

State of the art

compute Nth term after precomputation $\qquad d = \deg_y E(x,y)$

Method	char. 0	char. p
Binary powering ($d=1$)	$O(\log_2 N) + O(1)$	
Baby steps – Giant steps	$\widetilde{O}(\sqrt{N}) + O(1)$	✘
Divide and Conquer	✘	$O(\log_p N) \times \widetilde{O}(p^{3d})$

State of the art

compute Nth term after precomputation $d = \deg_y E(x,y)$

Method	char. 0	char. p
Binary powering ($d = 1$)	$O(\log_2 N) + O(1)$	
Baby steps – Giant steps	$\widetilde{O}(\sqrt{N}) + O(1)$	✘
Divide and Conquer	✘	$O(\log_p N) \times \widetilde{O}(p^{3d})$

Miller + Brown, 1966
An algorithm for evaluation of remote terms in a linear recurrence sequence

Fiduccia, 1985
An efficient formula for linear recurrences

State of the art

compute Nth term after precomputation $d = \deg_y E(x,y)$

Method	char. 0	char. p
Binary powering ($d = 1$)	$O(\log_2 N) + O(1)$	
Baby steps – Giant steps	$\widetilde{O}(\sqrt{N}) + O(1)$	✘
Divide and Conquer	✘	$O(\log_p N) \times \widetilde{O}(p^{3d})$

algebraic equation ⟶ differential equation ⟶ linear recurrence

Chudnovsky + Chudnovsky, 1988
Approximations and complex multiplication according to Ramanujan

State of the art

compute Nth term after precomputation $\qquad d = \deg_y E(x,y)$

Method	char. 0	char. p
Binary powering ($d = 1$)	$O(\log_2 N) + O(1)$	
Baby steps – Giant steps	$\widetilde{O}(\sqrt{N}) + O(1)$	✘
Divide and Conquer	✘	$O(\log_p N) \times \widetilde{O}(p^{3d})$

algebraic equation $\longrightarrow$ Mahler equation $\longrightarrow$ DAC recurrence

Christol + Kamae + Mendès France + Rauzy, 1980
Suites algébriques, automates et substitutions

Allouche + Shallit, 1992
The ring of k-regular sequences

From algebraic equation to Mahler equation

Algebraic equation $y = 2x + 2xy + xy^2 + xy^3$

$p = 3$

$$\begin{array}{c} \\ 1 \\ y \\ y^2 \end{array} \begin{array}{cccc} y & y^3 & y^9 & y^{27} \\ \left[\begin{array}{cccc} 0 & 1 & \frac{1+2x^2+x^3}{x^3} & \frac{1+2x^2+x^3+2x^5+x^6+x^8+x^9+2x^{11}+x^{12}}{x^{12}} \\ 1 & \frac{1+x}{x} & \frac{1+x+2x^2+x^3+x^4}{x^4} & \frac{1+x+2x^2+x^3+x^4+2x^5+2x^6+2x^7+x^8+x^9+x^{10}+2x^{11}+x^{12}+x^{13}}{x^{13}} \\ 0 & 2 & 2\,\frac{1+x+2x^2+x^3}{x^3} & \frac{2+2x+x^2+2x^3+2x^4+x^5+x^6+x^7+2x^8+2x^9+2x^{10}+x^{11}+2x^{12}}{x^{12}} \end{array}\right] \end{array}$$

Mahler equation

$$\left(2x^2 + 2x^3 + x^4\right) f(x) + \left(1 + x^2 + 2x^3 + 2x^4 + x^5 + 2x^6\right) f(x)^3 + \left(2 + 2x^3 + 2x^5 + x^6 + 2x^9\right) f(x)^9 + x^9 f(x)^{27} = 0$$

From algebraic equation to Mahler equation

Algebraic equation $y = 2x + 2xy + xy^2 + xy^3$

$p = 3$

$$\begin{array}{c} \\ 1 \\ y \\ y^2 \end{array} \begin{array}{cccc} y & y^3 & y^9 & y^{27} \\ \end{array}$$

$$\begin{array}{c|cccc} & y & y^3 & y^9 & y^{27} \\ \hline 1 & 0 & 1 & \frac{1+2x^2+x^3}{x^3} & \frac{1+2x^2+x^3+2x^5+x^6+x^8+x^9+2x^{11}+x^{12}}{x^{12}} \\ y & 1 & \frac{1+x}{x} & \frac{1+x+2x^2+x^3+x^4}{x^4} & \frac{1+x+2x^2+x^3+x^4+2x^5+2x^6+2x^7+x^8+x^9+x^{10}+2x^{11}+x^{12}+x^{13}}{x^{13}} \\ y^2 & 0 & 2 & 2\frac{1+x+2x^2+x^3}{x^3} & \frac{2+2x+x^2+2x^3+2x^4+x^5+x^6+x^7+2x^8+2x^9+2x^{10}+x^{11}+2x^{12}}{x^{12}} \end{array}$$

Mahler equation

$$\left(2x^2+2x^3+x^4\right)f(x) + \left(1+x^2+2x^3+2x^4+x^5+2x^6\right)f(x^3) + \left(2+2x^3+2x^5+x^6+2x^9\right)f(x^9) + x^9 f(x^{27}) = 0$$

Frobenius $f(x)^p = f(x^p)$

From Mahler equation to DAC recurrence

Algebraic equation $y = 2x + 2xy + xy^2 + xy^3$

Mahler equation $x^s f(x^q)$

$$\left(2x^2 + 2x^3 + x^4\right) f(x) + \left(1 + x^2 + 2x^3 + 2x^4 + x^5 + 2x^6\right) f(x^3) + \left(2 + 2x^3 + 2x^5 + x^6 + 2x^9\right) f(x^9) + x^9 f(x^{27}) = 0$$

Divide-and-conquer recurrence $f_{\frac{n-s}{q}}$

$$2f_{n-2} + 2f_{n-3} + f_{n-4} + f_{\frac{n}{3}} + f_{\frac{n-2}{3}} + 2f_{\frac{n-3}{3}} + 2f_{\frac{n-4}{3}} + f_{\frac{n-5}{3}} + 2f_{\frac{n-6}{3}} + 2f_{\frac{n}{9}} + 2f_{\frac{n-3}{9}} + 2f_{\frac{n-5}{9}} + f_{\frac{n-6}{9}} + 2f_{\frac{n-9}{9}} + f_{\frac{n-9}{27}} = 0$$

$f_x = 0$ if $x \notin \mathbb{N}_{\geq 0}$

From Mahler equation to DAC recurrence

Algebraic equation $y = 2x + 2xy + xy^2 + xy^3$

Mahler equation $x^s f(x^q)$

$$\left(2x^2 + 2x^3 + x^4\right) f(x) + \left(1 + x^2 + 2x^3 + 2x^4 + x^5 + 2x^6\right) f(x^3) + \left(2 + 2x^3 + 2x^5 + x^6 + 2x^9\right) f(x^9) + x^9 f(x^{27}) = 0$$

Divide-and-conquer recurrence $f_{\frac{n-s}{q}}$

$$2f_{n-2} + \cancel{2f_{n-3}} + \cancel{f_{n-4}} + f_{\frac{n}{3}} + f_{\frac{n-2}{3}} + 2f_{\frac{n-3}{3}} + 2f_{\frac{n-4}{3}} + f_{\frac{n-5}{3}} + 2f_{\frac{n-6}{3}} + 2f_{\frac{n}{9}} + 2f_{\frac{n-3}{9}} + 2f_{\frac{n-5}{9}} + f_{\frac{n-6}{9}} + 2f_{\frac{n-9}{9}} + f_{\frac{n-9}{27}} = 0$$

$f_x = 0$ if $x \notin \mathbb{N}_{\geq 0}$

From algebraic equation to DAC recurrence

$$+5x^{131}+2x^{130}+4x^{129}+x^{128}+2x^{127}+5x^{126}+3x^{125}+2x^{124}+4x^{123}+x^{122}+x^{121}+6x^{120}+6x^{119}$$

$$+2x^{118}+2x^{117}+5x^{116}+3x^{115}+6x^{114}+4x^{113}+2x^{112}+6x^{111}+4x^{110}+6x^{109}+5x^{108}+6x^{107}$$

$$+5x^{106}+6x^{105}+4x^{104}+3x^{103}+4x^{102}+x^{101}+2x^{100}+5x^{99}+3x^{98}+4x^{97}+5x^{71}+4x^{69}+2x^{68}+2x^{67}$$

$$+4x^{66}+5x^{65}+3x^{64}+x^{62}+2x^{57}+3x^{55}+3x^{54}+3x^{53}+6x^{52}+4x^{51}+5x^{50}+4x^{48}+2x^{46}+4x^{45}$$

$$+3x^{44}+x^{43}+6x^{42}+5x^{41}+2x^{40}+5x^{39}+3x^{38}+6x^{37}+3x^{36}+2x^{35}+x^{34}+4x^{33}+3x^{32}+6x^{31}+5x^{30}$$

$$+3x^{29}+4x^{28}+x^{27}+3x^{26}+6x^{25}+5x^{24}+5x^{23}+5x^{22}+2x^{21}+4x^{20}+x^{18}+2x^{17}+5x^{16}+5x^{15}+3x^{14}$$

$$+4x^{13}+6x^{12}+2x^{11}+4x^{10}+2x^{9}+x^{8}+2x^{7}+5x^{6}+5x^{4}+3x^{3}+4x^{2}+1\Big)f(x^{7})$$

$$+\Big(6x^{165}+5x^{164}+2x^{163}+2x^{162}+4x^{161}+3x^{160}+2x^{155}+3x^{153}+2x^{151}+4x^{150}+3x^{149}+6x^{147}$$

$$+x^{144}+2x^{143}+5x^{142}+4x^{141}+3x^{140}+6x^{139}+x^{137}+2x^{136}+5x^{135}+x^{134}+3x^{133}+5x^{132}+2x^{130}$$

$$+4x^{129}+3x^{128}+4x^{127}+6x^{126}+6x^{125}+6x^{123}+5x^{122}+2x^{121}+2x^{120}+4x^{119}+3x^{118}+5x^{116}$$

$$+3x^{115}+4x^{114}+4x^{113}+x^{112}+6x^{111}+4x^{106}+6x^{104}+4x^{102}+x^{101}+6x^{100}+5x^{98}+2x^{71}+3x^{69}$$

$$+x^{67}+2x^{66}+5x^{65}+5x^{64}+3x^{63}+4x^{62}+5x^{57}+4x^{55}+5x^{53}+3x^{52}+4x^{51}+x^{49}+5x^{46}+3x^{45}+4x^{44}$$

$$+6x^{43}+x^{42}+2x^{41}+5x^{39}+3x^{38}+4x^{37}+5x^{36}+x^{35}+4x^{34}+3x^{32}+6x^{31}+x^{30}+6x^{29}+2x^{28}+2x^{27}$$

$$+2x^{25}+4x^{24}+3x^{23}+6x^{21}+6x^{18}+5x^{17}+2x^{16}+2x^{15}+4x^{14}+3x^{13}+2x^{8}+3x^{6}+2x^{4}+4x^{3}+3x^{2}+6\Big)f(x^{49})$$

$$+\Big(x^{165}+2x^{164}+5x^{163}+5x^{162}+3x^{161}+4x^{160}+5x^{155}+4x^{153}+5x^{151}+3x^{150}+4x^{149}+x^{147}\Big)f(x^{343})=0$$

$O(\log_p N)\times p^{3d}$

Nth coefficient using section operators

Section operators

$$f(x) = \sum_{n \geq 0} f_n x^n \in \mathbb{K}[[x]]$$

$$S_r f(x) = \sum_{k \geq 0} f_{pk+r} x^k, \qquad 0 \leq r < p$$

Nth coefficient using section operators

Section operators

$$f(x) = \sum_{n \geq 0} f_n x^n \in \mathbb{K}[[x]]$$

$$S_r f(x) = \sum_{k \geq 0} f_{pk+r} x^k, \qquad 0 \leq r < p$$

Lemma

Let $f = \sum_{n \geq 0} f_n x^n$ *be in* $\mathbb{K}[[x]]$ *and let* $N = (N_\ell \cdots N_1 N_0)_p$ *be the radix* p *expansion of* N*. Then* $f_N = (S_{N_\ell} \cdots S_{N_1} S_{N_0} f)(0)$*.*

Nth coefficient using section operators

$$N = 100000 \qquad p = 7$$

$$= 5 \times 16807 + 6 \times 2401 + 4 \times 343 + 3 \times 49 + 5 \times 7 + 5 \times 1$$

$$= (5, 6, 4, 3, 5, 5)_7$$

$$f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + \cdots$$

$$S_5 f(x) = f_5 + f_{12} x + f_{19} x^2 + f_{26} x^3 + f_{33} x^4 + f_{40} x^5 + \cdots$$

$$S_5 S_5 f(x) = f_{40} + f_{89} x + f_{138} x^2 + f_{187} x^3 + f_{236} x^4 + f_{285} x^5 + \cdots$$

$$S_3 S_5 S_5 f(x) = f_{187} + f_{530} x + f_{873} x^2 + f_{1216} x^3 + f_{1559} x^4 + f_{1902} x^5 + \cdots$$

$$S_4 S_3 S_5 S_5 f(x) = f_{1559} + f_{3960} x + f_{6361} x^2 + f_{8762} x^3 + f_{11163} x^4 + \cdots$$

$$S_6 S_4 S_3 S_5 S_5 f(x) = f_{15965} + f_{32772} x + f_{49579} x^2 + f_{66386} x^3 + f_{83193} x^4 + \cdots$$

$$S_5 S_6 S_4 S_3 S_5 S_5 f(x) = f_{100000} + f_{217649} x + f_{335298} x^2 + f_{452947} x^3 + \cdots$$

$$S_5 S_6 S_4 S_3 S_5 S_5 f(0) = f_{100000}$$

Diagonal (forward)

$$F(x,y) = \frac{y(1-5xy-xy^2-3xy^3)}{1-2x-5xy-4xy^2-xy^3} = \qquad p = 7$$

y	$+2xy$	$+4x^2y$	$+x^3y$	$+2x^4y$	$+4x^5y$	$+x^6y$	$+2x^7y$	$+4x^8y$	$+x^9y$	$+2x^{10}y$
		$+3x^2y^2$	$+5x^3y^2$	$+x^4y^2$	$+5x^5y^2$	$+2x^6y^2$	$+2x^7y^2$		$+6x^9y^2$	$+3x^{10}y^2$
	$+3xy^3$		$+3x^3y^3$		$+6x^5y^3$	$+4x^6y^3$	$+x^7y^3$	$+6x^8y^3$		$+6x^{10}y^3$
	$+5xy^4$	$+6x^2y^4$		$+x^4y^4$	$+x^5y^4$		$+x^7y^4$	$+3x^8y^4$	$+5x^9y^4$	
		$+2x^2y^5$	$+2x^3y^5$		$+6x^5y^5$	$+4x^6y^5$	$+5x^7y^5$		$+4x^9y^5$	$+4x^{10}y^5$
		$+2x^2y^6$	$+3x^3y^6$	$+5x^4y^6$		$+5x^6y^6$	$+6x^7y^6$		$+4x^9y^6$	$+6x^{10}y^6$
		$+5x^2y^7$	$+6x^3y^7$		$+5x^5y^7$		$+6x^7y^7$		$+3x^9y^7$	$+5x^{10}y^7$
				$+2x^4y^8$	$+3x^5y^8$	$+2x^6y^8$		$+3x^8y^8$	$+6x^9y^8$	$+5x^{10}y^8$
			$+x^3y^9$	$+x^4y^9$	$+3x^5y^9$	$+6x^6y^9$	$+6x^7y^9$		$+x^9y^9$	$+6x^{10}y^9$
			$+5x^3y^{10}$		$+6x^5y^{10}$	$+2x^6y^{10}$		$+x^8y^{10}$		$+4x^{10}y^{10}$
				$+x^4y^{11}$	$+x^5y^{11}$	$+5x^6y^{11}$	$+4x^7y^{11}$	$+4x^8y^{11}$	$+2x^9y^{11}$	
					$+6x^5y^{12}$	$+2x^6y^{12}$	$+x^7y^{12}$		$+3x^9y^{12}$	$+3x^{10}y^{12}$
				$+5x^4y^{13}$		$+5x^6y^{13}$			$+3x^9y^{13}$	$+x^{10}y^{13}$
					$+5x^5y^{14}$		$+3x^7y^{14}$		$+4x^9y^{14}$	$+2x^{10}y^{14}$
					$+6x^5y^{15}$	$+x^6y^{15}$	$+3x^7y^{15}$	$+x^8y^{15}$	$+2x^9y^{15}$	$+4x^{10}y^{15}$
					$+5x^5y^{16}$	$+4x^6y^{16}$	$+4x^7y^{16}$		$+5x^9y^{16}$	$+4x^{10}y^{16}$

$$f(x) = DF(x) = 2x + 3x^2 + 3x^3 + x^4 + 6x^5 + 5x^6 + 6x^7 + 3x^8 + x^9 + 4x^{10} + \cdots$$

Diagonal (backward)

Theorem (Furstenberg's theorem)

Every algebraic series is the diagonal of a bivariate rational function.

$$E(x, f(x)) = 0, \quad f(0) = 0, \quad E_y(0,0) \neq 0$$

$$f(x) = D\frac{a}{b} \qquad \text{with} \quad a(x,y) = yE_y(xy,y), \quad b(x,y) = E(xy,y)/y$$

Furstenberg, 1967,
Algebraic functions over finite fields

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f$$

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f = S_r D \frac{a}{b} \qquad \text{diagonal}$$

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f = S_r D \frac{a}{b}$$

diagonal

↓

bivariate sections S_r: action on bivariate rational functions

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f = S_r D \frac{a}{b}$$ diagonal

↓

bivariate sections S_r: action on bivariate rational functions

$$S_r D \frac{a}{b} = D S_r \frac{a}{b}$$ commutation rule

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f = S_r D \frac{a}{b} \qquad \text{diagonal}$$

$\downarrow$

bivariate sections S_r: action on bivariate rational functions

$$S_r D \frac{a}{b} = D S_r \frac{a}{b} \qquad \text{commutation rule}$$

$\downarrow$

pseudo-sections T_r: action on bivariate polynomials

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f = S_r D\frac{a}{b}$$ diagonal

↓

bivariate sections S_r: action on bivariate rational functions

$$S_r D\frac{a}{b} = D S_r \frac{a}{b}$$ commutation rule

↓

pseudo-sections T_r: action on bivariate polynomials

$$S_r f = D S_r \frac{a}{b} = D\frac{S_r a b^{p-1}}{b}$$ Frobenius

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f = S_r D \frac{a}{b}$$ diagonal

↓

bivariate sections S_r: action on bivariate rational functions

$$S_r D \frac{a}{b} = D S_r \frac{a}{b}$$ commutation rule

↓

pseudo-sections T_r: action on bivariate polynomials

$$S_r f = D S_r \frac{a}{b} = D \frac{S_r a b^{p-1}}{b} = D \frac{T_r a}{b}$$ Frobenius

$$T_r v = S_r v b^{p-1}$$

Sections are diagonals

univariate sections S_r: action on algebraic formal series

$$S_r f = S_r D \frac{a}{b}$$ diagonal

$\downarrow$

bivariate sections S_r: action on bivariate rational functions

$$S_r D \frac{a}{b} = D S_r \frac{a}{b}$$ commutation rule

$\downarrow$

pseudo-sections T_r: action on bivariate polynomials

$$S_r f = D S_r \frac{a}{b} = D \frac{S_r a b^{p-1}}{b} = D \frac{T_r a}{b}$$ Frobenius

$$T_r v = S_r v b^{p-1}$$

Christol, 1979,
Ensembles presque périodiques k-reconnaissables

Nth coefficient using pseudo-section operators

univariate sections S_r: action on formal series

$$f_N = (S_{N_\ell} \cdots S_{N_1} S_{N_0} f)(0)$$

$$\downarrow$$

bivariate sections S_r: action on bivariate rational functions

$$\downarrow$$

pseudo-sections T_r: action on bivariate polynomials

$$f_N = \frac{(T_{N_\ell} \cdots T_{N_1} T_{N_0} a)(0,0)}{b(0,0)}$$

Nth coefficient using pseudo-section operators

univariate sections S_r: action on formal series

$$f_N = (S_{N_\ell} \cdots S_{N_1} S_{N_0} f)(0)$$

$$\downarrow$$

bivariate sections S_r: action on bivariate rational functions

$$\downarrow$$

pseudo-sections T_r: action on bivariate polynomials

$$f_N = \frac{(T_{N_\ell} \cdots T_{N_1} T_{N_0} a)(0,0)}{b(0,0)}$$

Finite dimensional stable subspace

$$T_r v = S_r v b^{p-1} \qquad B = b^{p-1}$$

Finite dimensional stable subspace

$$T_r v = S_r v b^{p-1} \qquad\qquad B = b^{p-1}$$

$$d_x = \max(\deg_x a, \deg_x b), \qquad d_y = \max(\deg_y a, \deg_y b)$$

$$\begin{array}{rcl} & \xrightarrow{\qquad\qquad\qquad T_r \qquad\qquad\qquad} & \\ \mathbb{F}_p[x,y]_{d_x,d_y} \longrightarrow & \mathbb{F}_p[x,y] \longrightarrow & \mathbb{F}_p[x,y] \\ v \longmapsto & vb^{p-1} = vB \longmapsto & S_r v B = T_r v \end{array}$$

Finite dimensional stable subspace

$$T_r v = S_r v b^{p-1} \qquad\qquad B = b^{p-1}$$

$$d_x = \max(\deg_x a, \deg_x b), \qquad d_y = \max(\deg_y a, \deg_y b)$$

$$\begin{array}{ccccc} & & \xrightarrow{\hspace{6em} T_r \hspace{6em}} & & \\ \mathbb{F}_p[x,y]_{d_x,d_y} & \longrightarrow & \mathbb{F}_p[x,y] & \longrightarrow & \mathbb{F}_p[x,y] \\ v & \longmapsto & vb^{p-1} = vB & \longmapsto & S_r vB = T_r v \end{array}$$

$\mathbb{F}_p[x,y]_{d_x,d_y}$ stable by the T_r

A geometrical evidence

$$\begin{array}{ccccc} & & \xrightarrow{\qquad\qquad\qquad T_r \qquad\qquad\qquad} & & \\ \mathbb{F}_p[x,y]_{d_x,d_y} & \longrightarrow & \mathbb{F}_p[x,y]_{pd_x,pd_y} & \longrightarrow & \mathbb{F}_p[x,y]_{d_x,d_y} \\ v & \longmapsto & vb^{p-1} = vB & \longmapsto & S_r vB = T_r v \end{array}$$

$p = 11$

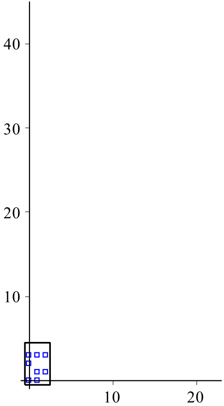
$E = (1+x)(x-y) + x^2y^2 + (1+x)y^3 + y^4$

$a = -y - xy^2 + 3y^3 + 4y^4 + 3xy^4 + 2x^2y^4$

$b = -1 + x - xy + y^2 + x^2y + y^3 + xy^3 + x^2y^3$

$d_x = 2,\ d_y = 4$

small box $[0, d_x] \times [0, d_y]$



A geometrical evidence

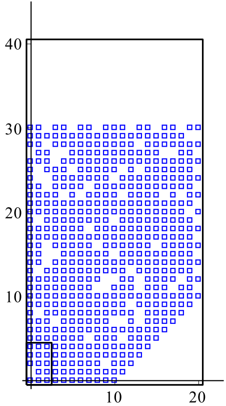
$$\xrightarrow{\hspace{10em} T_r \hspace{10em}}$$

$$\begin{array}{rcccc} \mathbb{F}_p[x,y]_{d_x,d_y} & \longrightarrow & \mathbb{F}_p[x,y]_{pd_x,pd_y} & \longrightarrow & \mathbb{F}_p[x,y]_{d_x,d_y} \\ v & \longmapsto & vb^{p-1} = vB & \longmapsto & S_r vB = T_r v \end{array}$$

dilation with ratio $p-1$

large box $[0,(p-1)d_x] \times [0,(p-1)d_y]$

$B = b^{p-1}$



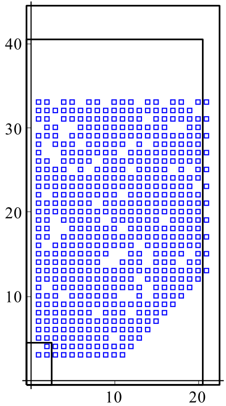
A geometrical evidence

$$\begin{array}{ccccc} & & \xrightarrow{\qquad\qquad\qquad T_r \qquad\qquad\qquad} & & \\ \mathbb{F}_p[x,y]_{d_x,d_y} & \longrightarrow & \mathbb{F}_p[x,y]_{pd_x,pd_y} & \longrightarrow & \mathbb{F}_p[x,y]_{d_x,d_y} \\ v & \longmapsto & vb^{p-1} = vB & \longmapsto & S_r vB = T_r v \end{array}$$

$v = xy^3$ in the canonical basis

translation by $(1, 3)$

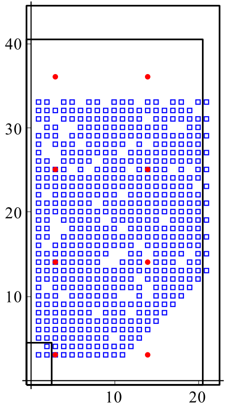
very large box $[0, pd_x] \times [0, pd_y]$ xy^3B



A geometrical evidence

$$\xrightarrow{\qquad\qquad\qquad\qquad T_r \qquad\qquad\qquad\qquad}$$

$$\begin{array}{ccccc} \mathbb{F}_p[x,y]_{d_x,d_y} & \longrightarrow & \mathbb{F}_p[x,y]_{pd_x,pd_y} & \longrightarrow & \mathbb{F}_p[x,y]_{d_x,d_y} \\ v & \longmapsto & vb^{p-1} = vB & \longmapsto & S_r vB = T_r v \end{array}$$



filter $r = 3$

$xy^3 B$

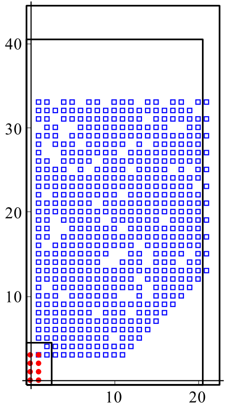
A geometrical evidence

$$\begin{array}{ccccc} & & \xrightarrow{\qquad\qquad T_r \qquad\qquad} & & \\ \mathbb{F}_p[x,y]_{d_x,d_y} & \longrightarrow & \mathbb{F}_p[x,y]_{pd_x,pd_y} & \longrightarrow & \mathbb{F}_p[x,y]_{d_x,d_y} \\ v & \longmapsto & vb^{p-1} = vB & \longmapsto & S_r vB = T_r v \end{array}$$

contraction

small box $[0, d_x] \times [0, d_y]$

$T_3 xy^3 = S_3 xy^3 B$



A geometrical evidence

$$\begin{array}{ccccc} & & \xrightarrow{\qquad\qquad\qquad T_r \qquad\qquad\qquad} & & \\ \mathbb{F}_p[x,y]_{d_x,d_y} & \longrightarrow & \mathbb{F}_p[x,y]_{pd_x,pd_y} & \longrightarrow & \mathbb{F}_p[x,y]_{d_x,d_y} \\ v & \longmapsto & vb^{p-1} = vB & \longmapsto & S_r vB = T_r v \end{array}$$

We can compute f_N in $O((d_x d_y)^2 \log N)$
if we know the matrices
$A_0, A_1, \ldots, A_{p-1}$
of
$T_0, T_1, \ldots, T_{p-1}$
in the canonical basis $(x^n y^m)$ of $\mathbb{F}_p[x,y]_{d_x,d_y}$.

Precomputation of $A_0, A_1, \dots, A_{p-1}$

All information is in $B = b^{p-1}$.

matrix A_r: $x^n y^m \xrightarrow[\text{translation}]{} x^n y^m B \xrightarrow[\text{selection}]{} S_r x^n y^m B$

No computation in $\mathbb{K} = \mathbb{F}_p$, except raising b to the power $p-1$

Cost: $\widetilde{O}(p^2)$ (binary powering, Kronecker substitution, FFT)

Theorem

The Nth coefficient can be computed in time

$$\widetilde{O}(p^2) + O(\log_p N).$$

Precomputation of $A_0, A_1, \ldots, A_{p-1}$

All information is in $B = b^{p-1}$.

$$\text{matrix } A_r\text{: } x^n y^m \xrightarrow[\text{translation}]{\hspace{3cm}} x^n y^m B \xrightarrow[\text{selection}]{\hspace{3cm}} S_r x^n y^m B$$

No computation in $\mathbb{K} = \mathbb{F}_p$, except raising b to the power $p-1$

Cost: $\widetilde{O}(p^2)$ (binary powering, Kronecker substitution, FFT)

Theorem

The N*th coefficient can be computed in time*

$$\widetilde{O}(p^2) + O(\log_p N).$$

To be compared with
$\widetilde{O}(p^{3d}) \times O(\log_p N)$

Only a small part of $B = b^{p-1}$ is enough

Task: Computation of A_0, A_1, …, A_{p-1}

row index $i = (k, \ell)$
column index $j = (n, m)$

$$B = \sum_{\alpha,\beta} c_{\alpha,\beta} x^\alpha y^\beta$$

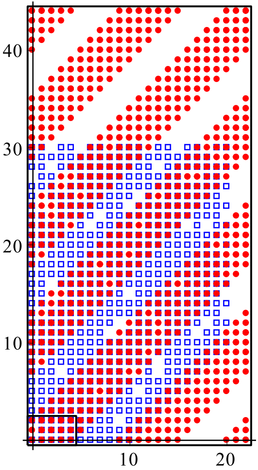
$$x^n y^m \xrightarrow[\text{translation}]{} x^n y^m B \xrightarrow[\text{selection}]{} S_r x^n y^m B$$

$$x^n y^m \longrightarrow \sum_{\alpha,\beta} c_{\alpha,\beta} x^{n+\alpha} y^{m+\beta} \longrightarrow \sum_{\substack{\alpha,\beta \\ (C)}} c_{\alpha,\beta} x^k y^\ell$$

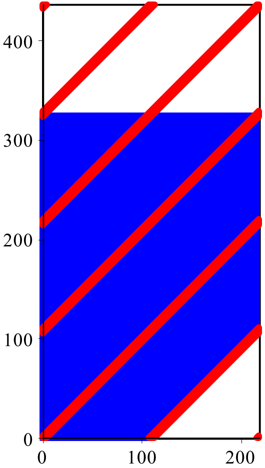
$$(C) \begin{cases} n + \alpha = pk + r \\ m + \beta = p\ell + r \end{cases} \Longrightarrow \beta = \alpha + p(\ell - k) + n - m$$

Only a small part of $B = b^{p-1}$ is enough

$p = 11$



$p = 109$



Improved precomputation

$$B(x/t, t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^{\alpha} t^{\beta-\alpha} = \sum_{\delta} \pi_{\delta}(x) t^{\delta}$$

Improved precomputation

$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^{\alpha} t^{\beta-\alpha} = \sum_{\delta} \pi_{\delta}(x) t^{\delta}$$

Frobenius

$$B(x/t,t) = b(x/t,t)^{p-1} = \frac{b(x/t,t)^p}{b(x/t,t)} = \frac{1}{b(x/t,t)} \times b(x^p/t^p, t^p)$$

Improved precomputation

$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^{\alpha} t^{\beta-\alpha} = \sum_{\delta} \pi_{\delta}(x) t^{\delta}$$

$$B(x/t,t) = b(x/t,t)^{p-1} = \frac{b(x/t,t)^p}{b(x/t,t)} = \frac{1}{b(x/t,t)} \times b(x^p/t^p, t^p)$$

$$\frac{1}{b(x/t,t)} = \sum_u c_u(x) t^u$$

rational series

Improved precomputation

$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^\alpha t^{\beta-\alpha} = \sum_\delta \pi_\delta(x) t^\delta$$

$$B(x/t,t) = b(x/t,t)^{p-1} = \frac{b(x/t,t)^p}{b(x/t,t)} = \frac{1}{b(x/t,t)} \times b(x^p/t^p, t^p)$$

$$\frac{1}{b(x/t,t)} = \sum_u c_u(x) t^u \qquad\qquad b(x^p/t^p,t^p) = \textstyle\sum_v b_v(x^p) t^{pv}$$

rational series

for free

Improved precomputation

$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^{\alpha} t^{\beta-\alpha} = \sum_{\delta} \pi_{\delta}(x) t^{\delta}$$

$$B(x/t,t) = b(x/t,t)^{p-1} = \frac{b(x/t,t)^p}{b(x/t,t)} = \frac{1}{b(x/t,t)} \times b(x^p/t^p, t^p)$$

$$\frac{1}{b(x/t,t)} = \sum_{u} c_u(x) t^u \qquad b(x^p/t^p, t^p) = \textstyle\sum_v b_v(x^p) t^{pv}$$

rational series

for free

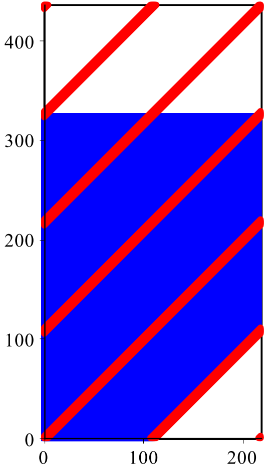
$$\pi_{\delta}(x) = \sum_{u+pv=\delta} c_u(x) b_v(x^p)$$

Improved precomputation

$\delta = \beta - \alpha =$ intercept of the strips with the vertical axis

big leaps from one strip to the next $\widetilde{O}(p)$:

- Kronecker substitution
- FFT
- Newton iteration



Main result

Theorem

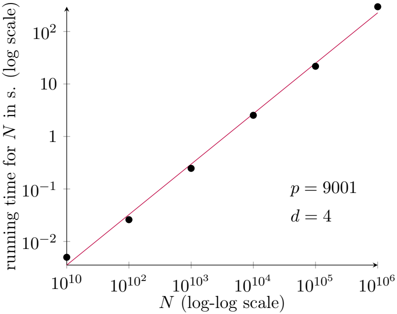
Let E be in $\mathbb{F}_p[x,y]_{h,d}$ satisfy $E(0,0)=0$ and $E_y(0,0)\neq 0$, and let $f\in\mathbb{F}_p[[x]]$ be its unique root with $f(0)=0$. One can compute the coefficient f_N of f in

$$\widetilde{O}(h(d+h)^5 p) + O(h^2(d+h)^2 \log_p N)$$

operations in $\mathbb{F}_p$.

Timings

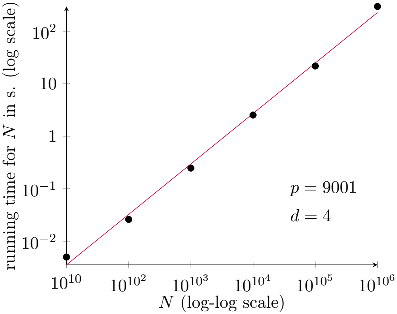
Maple implementation; timings on Intel Core i5, 2.8 GHz, 3MB.



$$\log \text{running time}(N) = \log \log N + C$$

Timings

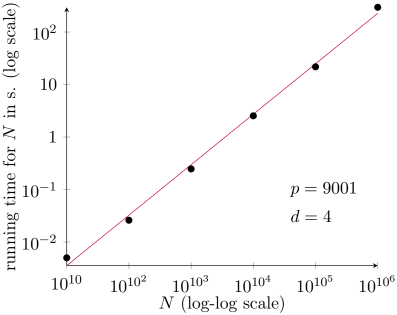
Maple implementation; timings on Intel Core i5, 2.8 GHz, 3MB.

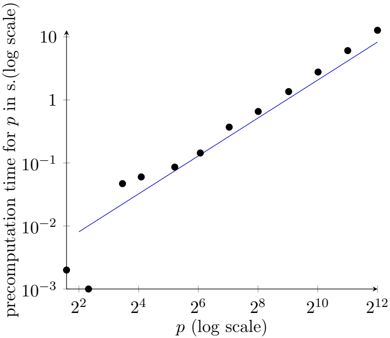


$$\log \text{running time}(N) = \log\log N + C$$
$$\text{running time}(N) = K \log N$$

Timings

Maple implementation; timings on Intel Core i5, 2.8 GHz, 3MB.



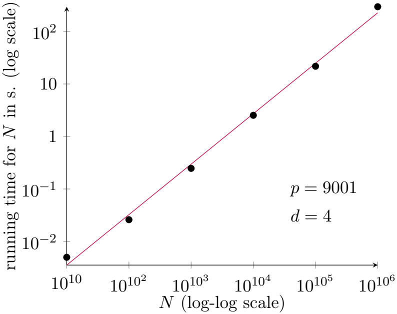


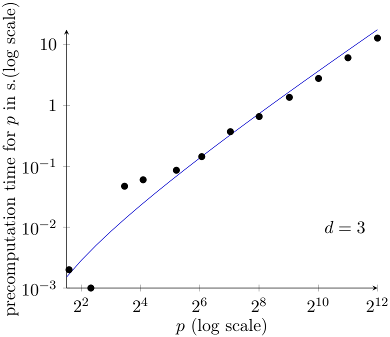
running time$(N) = K \log N$

precomputation time$(p) = Kp$

Timings

Maple implementation; timings on Intel Core i5, 2.8 GHz, 3MB.



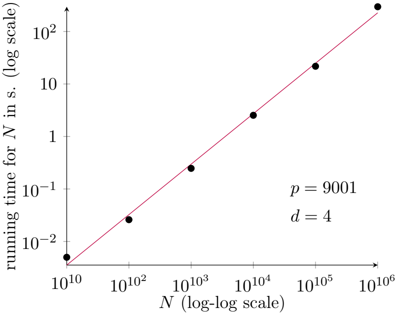


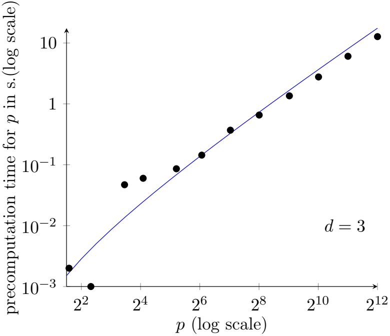
running $\text{time}(N) = K \log N$

precomputation $\text{time}(p) = Kp \log p$

Timings

Maple implementation; timings on Intel Core i5, 2.8 GHz, 3MB.





$O(\log N)$ $\widetilde{O}(p)$

Theorem

Let E be in $\mathbb{F}_p[x,y]_{h,d}$ satisfy $E(0,0)=0$ and $E_y(0,0)\neq 0$, and let $f \in \mathbb{F}_p[[x]]$ be its unique root with $f(0)=0$. One can compute the coefficient f_N of f in

$$\widetilde{O}(h(d+h)^5 p) + O(h^2(d+h)^2 \log_p N)$$

operations in $\mathbb{F}_p$.

Thanks for your attention!